J. Austral. Math. Soc. **23** (Series A) (1977), 202–206.

ON DOUBLY TRANSITIVE PERMUTATION GROUPS OF DEGREE PRIME SQUARED PLUS ONE

DAVID CHILLAG

(Received 22 March 1976; revised 1 June 1976)

Abstract

A doubly transitive permutation group of degree p^2+1, p a prime, is proved to be doubly primitive for $p \neq 2$. We also show that if such a group is not triply transitive then either it is a normal extension of $PSL(2,p^2)$ or the stabilizer of a point is a rank 3 group.

We will show that the groups described in the title are doubly primitive for $p > 2$ and sometimes they are even triply transitive.

THEOREM A. *Let G be a doubly transitive permutation group of degree p^2+1, p a prime. Then either G is doubly primitive or $p=2$ and G is the Frobenius group of order* 20.

THEOREM B. *Let G be a doubly transitive permutation group of degree p^2+1, p an odd prime. Assume that G_α contains two distinct Sylow p-subgroups. Then either a) G is triply transitive, or b) The stabilizer of a point is primitive rank 3 group of degree p^2 and subdegrees 1, $2(p-1)$, $(p-1)^2$. Moreover, the stabilizer of a point is isomorphic to a subgroup of $S_p \int S_2$, the wreath product of the symmetric groups of degrees p and* 2.

Groups described in b) are discussed in Higman (1970).

COROLLARY: *Let G be a doubly transitive permutation group of degree p^2+1, p a prime. Then one of the following is true*:

(*a*) *G is 3-transitive,*

(*b*) *$PSL(2,p^2) \subseteq G \subseteq P\Gamma L(2,p^2)$ in its natural representation,*

(*c*) *G is a Frobenius group of order 20 and $p=2$,*

(*d*) *The stabilizer of a point is primitive rank 3 group of degree p^2 and subdegrees 1, $2(p-1)$, $(p-1)^2$. Moreover, the stabilizer of a point is isomorphic to a subgroup of $S_p \int S_2$, the wreath product of the symmetric groups of degrees p and* 2.

NOTATIONS. We use notations of Wielandt (1964) for permutation groups and notations of Ryser (1963) for the parameters of a block design. If G acts on Ω and $T \subseteq G$ we define $F(T) = \{x \in \Omega \mid xt = x \text{ for all } t \in T\}$.

We start with the following lemma:

LEMMA. *Let G be a doubly transitive permutation group of degree $p^2 + 1$ on a set Ω. Here p is a prime. Then*:

a) *If $|G| \equiv 0(p^3)$ then G contains A_{p^2+1}.*

b) *There is no nontrivial block design with $\lambda = 1$ on Ω.*

c) *If G is sharply doubly transitive then $p = 2$ and $|G| = 20$.*

PROOF. Part a) is a result of Tsuzuku (1968), and part b) follows from the incidence equations of a block design and the Fisher inequality (see Ryser (1963)). In c) G contains a regular normal subgroup and if c) is not true, $p^2 + 1 = 2^x$ for some integer x. This is impossible since $p^2 + 1 \equiv 2(4)$.

PROOF OF THEOREM A. Assume that G is not doubly primitive. Let Ω be the set on which G acts and let $\alpha \in \Omega$. It follows that G_α has a complete system of inprimitivity sets on $\Omega - \{\alpha\}$. Let $\Lambda_0 = \{\Delta_1, \Delta_2, \cdots, \Delta_p\}$ be such a system and let $\Lambda = \Lambda_0 - \{\Delta_1\}$. Let $\beta \in \Delta_1$. We have that $|\Lambda_0| = p$. Let P be a Sylow p-subgroup of G contained in G_α. By the lemma, $|P| = p^2$. Let K be the kernel of the action of G_α on Λ_0 and let H be the stabilizer of Δ_1 in G_α in its action on Λ_0. Let A be the kernel of H on Δ_1. By the lemma we have that either $G_{\alpha\beta} \neq 1$ or we are done. Hence we can assume that $G_{\alpha\beta} \neq 1$. It follows that $H_\beta = G_{\alpha\beta} \neq 1$. Clearly H is transitive on Δ_1 and G_α is transitive on Λ_0. We can also assume that $p > 2$.

Since G_α/K is transitive permutation group of degree p, $|G_\alpha/K|_p = p$ so that $|K|_p = p$. Let P_0 be a Sylow p-subgroup of K. We can assume that $P_0 \subseteq P$. Since $|H : G_{\alpha\beta}| = p$ we get that $|A|_p = |G_{\alpha\beta}|_p = 1$. We use Wielandt (1964), 11.6, 11.7, without referring to them. First we prove that $A = 1$. Suppose $A \neq 1$. The lemma and lemma 1.1 of Praeger (submitted) implies that A fixes a point in some $\Delta_i \neq \Delta_1$. Thus A fixes at least two blocks of Λ_0 setwise. However H is either transitive or semiregular on Λ, and since its normal subgroup A fixes a block in Λ we get $A \subseteq K$. Since $|A|_p = 1$, $A \lhd K$ and K is transitive on each Δ_i we conclude that A is trivial on each Δ_i so that $A = 1$. This contradicts $A \neq 1$.

We now break the proof into two cases.

CASE 1. We assume that G_α/K is nonsolvable. It follows that G_α is doubly transitive on Λ. Since $H = G_{\alpha\beta}K$ we have that $G_{\alpha\beta}$ is transitive on Λ. The lemma and lemma 2 of Atkinson (1972/73) imply that $\Delta_1 - \{\beta\}$ is not $G_{\{\alpha,\beta\}}$-invariant. It follows that there exists a $G_{\alpha\beta}$-orbit Γ_0, on $\Delta_1 - \{\beta\}$ such that $\Gamma_0 g \not\subset \Delta_1$ for $g \in G_{\{\alpha,\beta\}} - G_{\alpha\beta}$. Set $\Gamma = \Gamma_0 g$ and $\Sigma = \{\Delta \in \Lambda \mid \Delta \cap \Gamma \neq \varnothing\}$. Since Σ is a $G_{\alpha\beta}$-orbit on Λ we get that $|\Sigma| = p - 1$ so that $\Gamma_0 = \Delta - \{\beta\}$ and $|\Delta \cap \Gamma| = 1$ for every $\Delta \in \Lambda$. If $K_\beta \neq 1$ then K_β fixes the point in $\Delta \cap \Gamma$ for all $\Delta \in \Lambda$ so that $|F(K_\beta)| > 2$. This contradicts our lemma because of B1 of O'Nan (1972).

Therefore $K_\beta = 1$. Since K is transitive on Δ_1 we have that $K = P_0$. Since $H \simeq H^{\Delta_1}$ and $K \lhd H$, H is metacyclic of order dividing $p(p-1)$, so that H/K is cyclic of order dividing $p-1$. This contradicts the assumption that G_α/K is nonsolvable. Thus we have:

Case 2. We assume that G_α/K is solvable. In this case G_α/K is a Frobenius group so that $G_{\alpha\beta}/K_\beta$ is semiregular on Λ. Let $t = |G_{\alpha\beta} : K_\beta|$. Then $t \mid p-1$. Since $P_0 \subseteq K \subseteq H$ and $|A|_p = 1$ we get that K is transitive on Δ_1 and therefore on each Δ_i.

Assume that K is not faithful on some $\Delta \in \Lambda_0$ and let M be the kernel of K on Δ. Since K is transitive on Δ, $|K : M|_p = p$ so that $|M|_p = 1$. Hence M cannot be transitive on any Δ_i, $1 \leqq i \leqq p$. Since $M \lhd K$ and $|\Delta_i| = p$ we get that M fixes all points of Ω. Since this is impossible, K is faithful on each Δ_i.

If $K_\beta = 1$ then $|G_{\alpha\beta}| = t$ and $|H| = tp$. Then H is solvable so that $G_{\alpha\beta}$ is semiregular on both $\Delta_1 - \{\beta\}$ and Λ. Hence $G_{\alpha\beta\gamma} = 1$ for $\gamma \in \Omega - \{\alpha,\beta\}$ and G is a Zassenhaus group of order $t(p^2+1)p^2$ where $t \mid p-1$. Since $p \neq 2$, this contradicts Feit (1960). Therefore $K_\beta \neq 1$.

By B 1 of O'Nan (1972), $F(K_\beta) = \{\alpha, \beta\}$. It follows that K_β fixes no point of Δ_2 so that K has at least two classes of subgroups of index p. This implies that K is nonsolvable and consequently K is doubly transitive on each Δ_i. By Theorem D of O'Nan (1975) we get that G is a normal extension of $PSL\,(n,q)$ for some $n \geqq 3$. This contradicts our lemma part b). Therefore the assumption that G is not doubly primitive is false and the theorem is proved.

Proof of Theorem B. Assume that G is not triply transitive. By Tsuzuku (1968), we can assume that $|G|_p = p^2$. Let Ω be the set on which G acts and let $\alpha, \beta \in \Omega, \alpha \neq \beta$. By assumption G_α contains two distinct Sylow p-subgroups. By Theorem A, G_α is primitive on $\Omega - \{\alpha\}$ and by assumption it is not doubly transitive. By Wielandt (1969), there is a subgroup N, of index 2 in G_α such that $N = X \times Y$, X, Y intransitive on $\Omega - \{\alpha\}$. Since G_α is primitive, N is transitive so that X and Y have, each, p orbits of size p on $\Omega - \{\alpha\}$. Let P be a Sylow p-subgroup of G contained in N; then we can write $P = P_1 \times P_2, P_1 \subseteq X, P_2 \subseteq Y, |P_1| = |P_2| = p$. If X is not faithful on one of its orbits the kernel on this orbit must be transitive on some other orbit or else the kernel would fix Ω. This implies that $|X|_p \geqq p^2$ which is impossible. Thus X is faithful on its orbits. The same is true for Y.

Let $\Lambda = \{\Lambda_i \mid 1 \leqq i \leqq p\}$ be the set of X-orbits on $\Omega - \{\alpha\}$ and let $\Gamma = \{\Gamma_i \mid 1 \leqq i \leqq p\}$ be the set of Y-orbits on $\Omega - \{\alpha\}$. Suppose X is solvable. Then $P_1 \lhd N$. Let $t \in G_\alpha - N$. Then $(P_1)^t \lhd N$ and if $(P_1)^t \neq P_1$ then $(P_1)^t P_1$ is a normal Sylow p-subgroup of N and therefore of G_α, contradicting the fact that G_α contains at least two Sylow p-subgroups. Thus $(P_1)^t = P_1$ and $P_1 \lhd G_\alpha$, contradicting the primitivity of G_α on $\Omega - \{\alpha\}$. We conclude that X is nonsolvable and therefore doubly transitive on each of its orbits. The same is true for Y.

Since Λ is a complete system of imprimitivity sets for the action of N on $\Omega - \{\alpha\}, N$ is transitive on Λ and therefore Y is transitive on Λ. If Y has a kernel, $V \neq 1$, on Λ then $|Y : V|_p = p$ and since $V \lhd Y$, V is either transitive or trivial on Γ_1. Since Y is faithful on Γ_1, V is transitive on it so that $|V|_p = p$. This implies that $p^2 \| |Y|$ which is impossible. Hence Y is faithful on Λ and since it is unsolvable, Y is doubly transitive on Λ. Certainly we can assume that $\Lambda_1 = \beta^X$ and $\Gamma_1 = \beta^Y$. Put $W = \{y \in Y \mid \Lambda_1 y = \Lambda_1\}$. Then $Y_\beta \subseteq W$ and since $|Y : Y_\beta| = |Y : W| = p$ we get that $W = Y_\beta$.

Hence Y_β is transitive on $\Lambda - \{\Lambda_1\}$. Since X is transitive on Λ_1 and $[X, Y_\beta] = 1$ we obtain that Y_β fixes Λ_1 pointwise. Thus $F(Y_\beta) = \Lambda_1 \cup \{\alpha\}$. By symmetry X_β is transitive on $\Gamma - \{\Gamma_1\}$ and $F(X_\beta) = \Gamma_1 \cup \{\alpha\}$. Now $p^2 = |N : N_\beta| = |X : X_\beta||Y : Y_\beta|$ implies that $N_\beta = X_\beta \times Y_\beta$. The previous paragraphs imply that $\Gamma_1 - \{\beta\}$, $\Lambda_1 - \{\beta\}$ and $(\bigcup_{i=1} \Lambda_i) - \Gamma_1 - \Lambda_1$ are the N_β-orbits on $\Omega - \{\alpha, \beta\}$. Their sizes are $p-1$, $p-1$, $(p-1)^2$ respectively. Also, Γ_1, contains one point from each Λ_i.

Since $|G_{\alpha\beta} : N_\beta| = 2$ we can choose $t \in G_{\alpha\beta} - N_\beta$. We have that $G_{\alpha\beta} = N_\beta \langle t \rangle$ and $G_\alpha = N\langle t \rangle$ because $t^2 \in N_\beta$. Suppose that t fixes both $\Gamma_1 - \{\beta\}$ and $\Lambda_1 - \{\beta\}$ as sets. Then $(X_\beta)^t$ acts on each of these sets and $(X_\beta)^t$ fixes $\Gamma_1 - \{\beta\}$ pointwise. Thus $(X_\beta)^t \cap Y_\beta = 1$ as Y is faithful on Γ_1. Since $(X_\beta)^t \subseteq N_\beta$ and $(X_\beta)^t$ fixes Γ_1 pointwise we have that $(X_\beta)^t$ acts trivially on Λ. Then $(X_\beta)^t$ is contained in the kernel of the action of N_β on Λ, namely X_β. Hence $(X_\beta)^t = X_\beta$.

Let $g \in G_\alpha$ and put $g = t^i h, h \in N$ for some integer i. Then since $X \lhd N, (X_\beta)^g \cap G_{\alpha\beta} = (X_\beta)^h \cap G_{\alpha\beta} \subseteq X \cap G_{\alpha\beta} = X_\beta$. Thus X_β is a strongly closed subgroup of $G_{\alpha\beta}$ in G_α. We now apply our lemma and B of O'Nan (1972) to get a contradiction.

Therefore t does not fix $\Gamma_1 - \{\beta\}$ and $\Lambda_1 - \{\beta\}$ and since t normalizes N_β, it must interchange these sets. We conclude that G_α is a rank 3 group on $\Omega - \{\alpha\}$ and the sizes of the $G_{\alpha\beta}$-orbits are 1, $2(p-1)$, $(p-1)^2$. Using Higman (1970) we are done.

We remark that the proof of Theorem B is also a proof for the following extension of Wielandt (1969):

THEOREM C. *Let G be a primitive but not doubly transitive permutation group of degree p^2. Assume that G_α contains two distinct Sylow p-subgroups. Then G is either rank 3 or rank 4 permutation group with sub-degrees* 1, $2(p-1),(p-1)^2$ or $1,(p-1),(p-1),(p-1)^2$.

In fact the rank 4 case does not occur because of Proposition 0.1 of Iwasaki (1973) that states that we are in case I and proposition 1.1 of Iwasaki (1973).

PROOF OF THE COROLLARY. By Theorems A and B and the lemma we can assume that $p \neq 2$, G_α contains a unique Sylow p-subgroup P and $|P| = p^2$. Now $P \lhd G_\alpha$ and since G_α is primitive, P is regular on $\Omega - \{\alpha\}$. By a result of Hering, Kantor and Seitz (1972) we get that G has a normal subgroup M such that $G \subsetneq \mathrm{Aut}(M)$, where M is either $PSL(2,p^2)$ or sharply 2-transitive, (because the degree is p^2+1). If M is sharply 2-transitive, so is G and $|G| = |M| = 20$ and $p = 2$. This proves the corollary.

Acknowledgement

I wish to thank Dr. Cheryl E. Praeger for her helpful suggestions.

References

M. D. Atkinson (1972/73), 'Two theorems on doubly transitive permutation groups', *J. London Math. Soc.* (2), **6**, 269–274.

Walter Feit (1960), 'On a class of doubly transitive permutation groups', *Illinois J. Math.* **4**, 170–186.

Christoph Hering, William M. Kantor and Gary M. Seitz (1972), 'Finite groups with a split BN — pair of rank 1, I', *J. Algebra* **20**, 435–475.

D. G. Higman (1970), 'Characterization of families of rank 3 permutation groups by the subdegrees. I', *Arch. der Math.* **21**, 151–156.

Shiro Iwasaki (1973), 'On finite permutation groups of rank 4', *J. Math., Kyoto Univ.* **13**, 1–20.

Michael O'Nan (1972), 'A characterization of $L_n(q)$ as a permutation group', *Math. Z.* **127**, 301–314.

Michael O'Nan (1975), 'Normal structure of the one point stabilizer of doubly transitive permutation group II', *Trans. Amer. Math. Soc.* **214**, 43–74.

Cheryl E. Praeger (submitted), 'Doubly transitive permutation groups which are not doubly primitive'.

Herbert John Ryser (1963), *Combinatorial Mathematics* (The Carus Mathematical Monographs, 14. Math. Assoc. Amer., Buffalo, New York; John Wiley & Sons, New York; 1963).

Tosiro Tsuzuku (1968), 'On doubly transitive permutation groups of degree $1+p+p^2$ where p is a prime number', *J. Algebra* **8**, 143–147.

Helmut Wielandt (1964), *Finite Permutation Groups* (translated by R. Bercov. Academic Press, New York, London, 1964).

Helmut W. Wielandt (1969), Permutation Groups Through Invariant Relations and Invariant Functions (Lecture Notes. Department of Mathematics, Ohio State University, Columbus, Ohio, 1969).

Technion,
Israel Institute of Technology,
Haifa, Israel.